



CalPERS Office of Audit Services
Audit Resolution Policy

Purpose In accordance with the Institute of Internal Auditors *International Standards for the Professional Practice of Internal Auditing (Standards)*, the Chief Auditor is required to establish a follow-up process to monitor audit findings and to ensure management actions have been effectively implemented or that executive staff has accepted the risk of not taking action.

Policy The policy provides a system to track corrective actions or acceptance of risk taken by management on reported audit issues and to convey these actions to executive staff and to the Risk and Audit Committee in keeping with the Board of Administration’s fiduciary oversight responsibilities.

Management has a responsibility to promptly evaluate reported audit findings, determine appropriate actions to best resolve outstanding items reported, and assure completion of the actions within an established timeframe. The resolution process is the follow-up phase of the audit to ensure that management actions have been effectively implemented or that executive staff has accepted the risk of not taking action.

Topic	Page
Internal Audits	2
Public Agency Reviews	5
Investment Program Audits	7
External Audits	8

Internal Audits

Internal Audits Defined

The internal audit team of the Office of Audit Services (OFAS) performs internal audits on compliance and the effectiveness and efficiency of CalPERS operations, systems, policies, and procedures. Internal audits also include audits of health maintenance organizations, third party administrators, and external providers of investment-related services.

Internal Audit Final Report

OFAS will transmit the final audit report to the respective division(s), executive staff, and the Risk and Audit Committee which includes management's written response outlining its planned corrective action for all findings and recommendations. OFAS monitors and reports quarterly on the resolution status of all findings to the appropriate division management and executive staff until fully resolved.

Resolution Options

Audit findings can be resolved in one of two ways.

- Division management implements the recommendation contained in the report.
 - Division management accepts the risk of not implementing corrective action due to cost or other considerations. Refer to Acceptance of Risk on page 3 of this policy.
-

Completion

The audited division shall notify OFAS when the recommendation contained in the final report has been implemented or acceptance of risk has been selected. OFAS shall perform tests as deemed necessary to ensure that management has implemented appropriate corrective action.

Division management that has oversight of health maintenance organizations, third-party administrators, or external providers of investment-related services shall be responsible for ensuring resolution of audit findings and determining if the corrective action has been implemented. OFAS will assess the reasonableness of the corrective action implemented prior to reporting the finding as resolved.

Continued on next page

Internal Audits, Continued

Findings Unresolved for Six Months

The Chief Auditor shall report findings unresolved for six months from the date of the final audit report to executive staff.

Findings Unresolved for One Year

When any findings remain unresolved for one year, the Deputy Executive Officer over the audited division shall be required to either:

- Provide a written explanation as to why the issue remains open and the corrective action plan to resolve the issue.
- Accept the risk of not implementing corrective action and provide a written explanation as to why the acceptance of risk is the most appropriate disposition of the issue. The steps outlined under Acceptance of Risk, as noted below, will apply.

The Chief Auditor shall report any findings that remain unresolved for one year to executive staff.

Acceptance of Risk

The audited division may accept the risk of not implementing corrective action, unless it violates the applicable laws and regulations, and provide a written explanation as to why the acceptance of risk is the most appropriate disposition of the issue. The explanation should include the cost benefit analysis of not implementing the recommendation and/or the mitigating controls in existence. The respective Deputy Executive Officer must approve and sign off on any proposed acceptance of risk.

The Chief Auditor shall then report the risk acceptance to the Chief Risk Officer and the Integrated Assurance Risk Council which includes executive staff and the General Counsel. The Chief Risk Officer shall track all accepted risks and include these risks in the enterprise risk monitoring process.

In accordance with the *Standards* and Government Code section 13887.5(a), if the Chief Auditor believes that management has accepted a level of risk that may be unacceptable to the organization, the Chief Auditor and the General Counsel must report the matter to the Risk & Audit Committee.

Continued on next page

Internal Audits, Continued

Report to Risk and Audit Committee The Chief Auditor shall provide quarterly status reports to the Risk and Audit Committee of the Board of Administration.

Public Agency Reviews

Public Agency Reviews Defined

The public agency team reviews public agencies (contracting public agencies, school districts, California State Universities, and State agencies) to ensure compliance with the Public Employees' Retirement Law, applicable regulations, and contractual provisions.

Public Agency Final Report

OFAS will issue a final report on the results of the public agency review to the subject agency, the appropriate divisions, and the Risk and Audit Committee. As part of the final report, the agency's written response will be included stating either concurrence or non-concurrence with all findings and recommendations as well as any explanatory comments.

Resolution Options

The public agency will work with Customer Services and Support (CSS) to take the necessary corrective actions to resolve the findings and bring the agency into compliance with the Public Employees' Retirement Law, applicable regulations, and its contractual provisions.

Audit findings can be resolved as follows:

- The public agency and CSS implement the recommendation contained in the report.
 - CSS management accepts the risk of not implementing corrective action due to other compensating controls or cost benefit analysis. Refer to Acceptance of Risk on page 6 of this policy.
-

Completion

CSS shall notify OFAS when the recommendation contained in the final report has been implemented or acceptance of risk has been selected. OFAS will review and verify that corrective action has been implemented as identified in the final audit report.

Continued on next page

Public Agency Reviews, Continued

Findings Unresolved for One Year

When any findings remain unresolved for one year, the CSS Deputy Executive Officer shall be required to either:

- Provide a written explanation as to why the issue remains open and a corrective action plan to resolve the issue.
- Accept the risk of not implementing corrective action and provide a written explanation as to why the acceptance of risk is the most appropriate disposition of the issue. The steps outlined under Acceptance of Risk, as noted below, will apply.

The Chief Auditor shall report any findings that remain unresolved for one year to executive staff.

Acceptance of Risk

CSS may accept the risk of not implementing corrective action, unless it violates the Public Employees Retirement Law, and provide a written explanation as to why the acceptance of risk is the most appropriate disposition of the issue. The explanation should include the cost benefit analysis of not implementing the recommendation and/or the mitigating controls in existence. The CSS Deputy Executive Officer must sign off on any proposed acceptance of risk.

The Chief Auditor shall then report the risk acceptance to the Chief Risk Officer and the Integrated Assurance Risk Council which includes executive staff and the General Counsel. The Chief Risk Officer shall track all accepted risks and include these risks in the enterprise risk monitoring process.

In accordance with the *Standards* and Government Code section 13887.5(a), if the Chief Auditor believes that management has accepted a level of risk that may be unacceptable to the organization, the Chief Auditor and the General Counsel must report the matter to the Risk and Audit Committee.

Report to Risk and Audit Committee

The Chief Auditor shall provide quarterly status reports to the Risk and Audit Committee of the Board of Administration.

Investment Program Audits

**Investment
Program
Audits
Defined**

OFAS engages external audit firms to perform agreed-upon procedures engagements with CalPERS general partners, advisors, and property managers. An agreed-upon procedures engagement, consistent with American Institute of Certified Public Accountants (AICPA) Attestation Standards, is one in which an external auditor is engaged by CalPERS to issue a report of findings based on specific procedures performed on a subject matter.

Final Report

The final report details findings, recommends corrective action, and includes the general partner, advisor, or property manager's response to the findings.

Responsibility

Program management shall be responsible for obtaining specific corrective actions from the general partner, advisor, or property manager to resolve the findings and completion dates for implementing those actions.

Program management shall be responsible for ensuring resolution of audit findings and ensuring that the general partner, advisor, or property manager implements property level corrections on a portfolio-wide basis as appropriate. Program management shall notify OFAS when the recommendation contained in the final report has been implemented or acceptance of risk has been selected. Refer to Acceptance of Risk on page 3 of this policy.

OFAS shall report findings that are not resolved within 12 calendar months to executive staff.

**Report to Risk
and Audit
Committee**

The Chief Auditor shall provide quarterly status reports to the Risk and Audit Committee of the Board of Administration.

External Audits

External Audits Defined Audits performed by CalPERS independent financial statement auditor and any other external audits that may occur.

Final Report The final report details findings, recommends corrective action, and includes management's response to the findings.

Responsibility

- Management is responsible for providing OFAS with specific corrective actions to resolve the findings and completion dates for implementing those actions.
- OFAS shall report to the Risk and Audit Committee the status of corrective actions on a quarterly basis.

Completion The applicable division shall notify OFAS when the division has implemented the recommendation contained in the report. OFAS will obtain and review information for audit finding closure and notify the external auditor. The external auditor shall perform tests as deemed necessary to ensure that management has implemented appropriate corrective action. OFAS shall report outstanding findings to executive staff at the Integrated Assurance Risk Council meetings and quarterly to the Risk and Audit Committee.

Report to Risk and Audit Committee The Chief Auditor shall provide quarterly status reports to the Risk and Audit Committee of the Board of Administration.
